

502 poc. 60 US00

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

JC978 U.S. PRO  
10/044110  
01/10/02

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2001年 1月15日

出 願 番 号

Application Number:

特願2001-006758

出 願 人

Applicant(s):

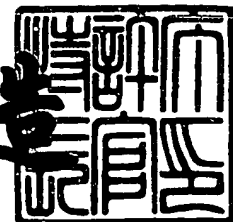
ソニー株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年11月30日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3104792

【書類名】 特許願

【整理番号】 0000962208

【提出日】 平成13年 1月15日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/56

【発明者】

    【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社  
                                内

    【氏名】 齋藤 真

【特許出願人】

    【識別番号】 000002185

    【氏名又は名称】 ソニー株式会社

【代理人】

    【識別番号】 100082131

    【弁理士】

    【氏名又は名称】 稲本 義雄

    【電話番号】 03-3369-6479

【手数料の表示】

    【予納台帳番号】 032089

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

    【物件名】 要約書 1

    【包括委任状番号】 9708842

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理装置および方法、記録媒体、並びにプログラム

【特許請求の範囲】

【請求項 1】 他の情報処理装置とネットワークを介して接続される情報処理装置において、

前記他の情報処理装置との通信が確立したとき、前記情報処理装置の最初の位置を特定する第 1 の位置情報、および、前記他の情報処理装置の最初の位置を特定する第 2 の位置情報を記憶する記憶手段と、

前記他の情報処理装置からデータを受信する受信手段と、

前記情報処理装置の現在の位置を特定する第 3 の位置情報を取得する取得手段と、

前記取得手段により取得された前記第 3 の位置情報が、前記記憶手段に記憶されている前記第 1 の位置情報に対応するか否かを判定する第 1 の判定手段と、

前記第 1 の判定手段による判定結果に基づいて、前記受信手段により受信された前記データを認証する認証手段と

を備えることを特徴とする情報処理装置。

【請求項 2】 前記第 1 の判定手段による判定の結果、前記第 3 の位置情報が前記第 1 の位置情報に対応しないと判定された場合、前記受信手段により受信された前記データに含まれる、送信先アドレスを構成する前記情報処理装置の第 4 の位置情報、および、送信元アドレスを構成する前記他の情報処理装置の第 5 の位置情報を読み取る読み取り手段と、

前記読み取り手段により読み取られた前記第 5 の位置情報が、前記記憶手段に記憶されている前記第 2 の位置情報に対応するか否かを判定する第 2 の判定手段と

をさらに備えることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】 前記第 1 の判定手段による判定の結果、前記第 3 の位置情報が前記第 1 の位置情報に対応しないと判定された場合、前記第 4 の位置情報を前記第 1 の位置情報により置換する置換手段をさらに備える

ことを特徴とする請求項 2 に記載の情報処理装置。

【請求項 4】 前記第 2 の判定手段による判定の結果、前記第 5 の位置情報が前記第 2 の位置情報に対応しないと判定された場合、前記第 5 の位置情報を前記第 2 の位置情報により置換する置換手段をさらに備える

ことを特徴とする請求項 2 に記載の情報処理装置。

【請求項 5】 前記第 4 の位置情報は、前記送信先アドレスの上位の一部のビットに割り当てられている

ことを特徴とする請求項 2 に記載の情報処理装置。

【請求項 6】 前記第 5 の位置情報は、前記送信元アドレスの上位の一部のビットに割り当てられている

ことを特徴とする請求項 2 に記載の情報処理装置。

【請求項 7】 前記認証手段は、前記受信手段により受信された前記データを認証するのに、さらに前記第 1 および第 2 の位置情報を用いる

ことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 8】 前記情報処理装置が他のネットワークに接続されたとき、前記情報処理装置の現在の位置を特定する第 4 の位置情報および前記情報処理装置を特定する識別情報を、前記ネットワークに接続されている情報蓄積装置に通知する通知手段をさらに備える

ことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 9】 前記識別情報は、前記ネットワーク上において、前記情報処理装置を特定する端末識別子である

ことを特徴とする請求項 8 に記載の情報処理装置。

【請求項 10】 前記他の情報処理装置との通信が切断されたとき、前記記憶手段に記憶されている前記第 1 および第 2 の位置情報をリセットするリセット手段をさらに備える

ことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 11】 他の情報処理装置とネットワークを介して接続される情報処理装置の情報処理方法において、

前記他の情報処理装置との通信が確立したとき、前記情報処理装置の最初の位置を特定する第 1 の位置情報、および、前記他の情報処理装置の最初の位置を特

定する第 2 の位置情報の記憶を制御する記憶制御ステップと、

前記他の情報処理装置からデータを受信する受信ステップと、

前記情報処理装置の現在の位置を特定する第 3 の位置情報を取得する取得ステップと、

前記取得ステップの処理により取得された前記第 3 の位置情報が、前記記憶制御ステップの処理により記憶が制御されている前記第 1 の位置情報に対応するかどうかを判定する判定ステップと、

前記第 1 の判定ステップの処理による判定結果に基づいて、前記受信ステップの処理により受信された前記データを認証する認証ステップと

を含むことを特徴とする情報処理方法。

【請求項 1 2】 他の情報処理装置とネットワークを介して接続される情報処理装置を制御するプログラムにおいて、

前記他の情報処理装置との通信が確立したとき、前記情報処理装置の最初の位置を特定する第 1 の位置情報、および、前記他の情報処理装置の最初の位置を特定する第 2 の位置情報の記憶を制御する記憶制御ステップと、

前記他の情報処理装置からデータを受信する受信ステップと、

前記情報処理装置の現在の位置を特定する第 3 の位置情報を取得する取得ステップと、

前記取得ステップの処理により取得された前記第 3 の位置情報が、前記記憶制御ステップの処理により記憶が制御されている前記第 1 の位置情報に対応するかどうかを判定する判定ステップと、

前記第 1 の判定ステップの処理による判定結果に基づいて、前記受信ステップの処理により受信された前記データを認証する認証ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項 1 3】 他の情報処理装置とネットワークを介して接続されるコンピュータに、

前記他の情報処理装置との通信が確立したとき、前記情報処理装置の最初の位置を特定する第 1 の位置情報、および、前記他の情報処理装置の最初の位置を特

定する第 2 の位置情報の記憶を制御する記憶制御ステップと、

前記他の情報処理装置からデータを受信する受信ステップと、

前記情報処理装置の現在の位置を特定する第 3 の位置情報を取得する取得ステップと、

前記取得ステップの処理により取得された前記第 3 の位置情報が、前記記憶制御ステップの処理により記憶が制御されている前記第 1 の位置情報に対応する可否かを判定する判定ステップと、

前記第 1 の判定ステップの処理による判定結果に基づいて、前記受信ステップの処理により受信された前記データを認証する認証ステップと

を実行させることを特徴とするプログラム。

【請求項 1 4】 他の情報処理装置とネットワークを介して接続される情報処理装置において、

前記他の情報処理装置との通信が確立したとき、前記情報処理装置の最初の位置を特定する第 1 の位置情報、および、前記他の情報処理装置の最初の位置を特定する第 2 の位置情報を記憶する記憶手段と、

前記情報処理装置の現在の位置を特定する第 3 の位置情報を取得する第 1 の取得手段と、

前記第 1 の取得手段により取得された前記第 3 の位置情報が、前記記憶手段に記憶されている前記第 1 の位置情報に対応する可否かを判定する第 1 の判定手段と、

前記他の情報処理装置の現在の位置を特定する第 4 の位置情報を取得する第 2 の取得手段と、

前記第 2 の取得手段により取得された前記第 4 の位置情報が、前記記憶手段に記憶されている前記第 2 の位置情報に対応する可否かを判定する第 2 の判定手段と、

前記第 1 および第 2 の判定手段の判定結果に基づいて、前記他の情報処理装置にデータを送信する送信手段と

を備えることを特徴とする情報処理装置。

【請求項 1 5】 前記第 1 の判定手段による判定の結果、前記第 3 の位置情

報が前記第1の位置情報に対応しないと判定された場合、前記第3の位置情報を前記第1の位置情報により置換する置換手段をさらに備える

ことを特徴とする請求項14に記載の情報処理装置。

【請求項16】 前記第2の判定手段による判定の結果、前記第4の位置情報が前記第2の位置情報に対応しないと判定された場合、前記第4の位置情報を前記第2の位置情報により置換する置換手段をさらに備える

ことを特徴とする請求項14に記載の情報処理装置。

【請求項17】 前記記憶手段に記憶されている前記第1および第2の位置情報を用いて、前記データに付加する付加情報を演算する演算手段と、

前記演算手段により演算された前記付加情報を前記データに付加する付加手段と

をさらに備え、

前記送信手段は、前記第1の取得手段により取得された前記第3の位置情報を送信元アドレスに設定するとともに、前記第2の取得手段により取得された前記第4の位置情報を送信先アドレスに設定して、前記付加手段により前記付加情報が付加された前記データを送信する

ことを特徴とする請求項14に記載の情報処理装置。

【請求項18】 前記第3の位置情報は、前記送信先アドレスの上位の一部のビットに割り当てられている

ことを特徴とする請求項17に記載の情報処理装置。

【請求項19】 前記第4の位置情報は、前記送信元アドレスの上位の一部のビットに割り当てられている

ことを特徴とする請求項17に記載の情報処理装置。

【請求項20】 前記情報処理装置が他のネットワークに接続されたとき、前記情報処理装置の現在の位置を特定する第5の位置情報および前記情報処理装置を特定する識別情報を、前記ネットワークに接続されている情報蓄積装置に通知する通知手段をさらに備える

ことを特徴とする請求項14に記載の情報処理装置。

【請求項21】 前記識別情報は、前記ネットワーク上において、前記情報

処理装置を特定する端末識別子である

ことを特徴とする請求項20に記載の情報処理装置。

【請求項22】 前記他の情報処理装置との通信が切断されたとき、前記記憶手段に記憶されている前記第1および第2の位置情報をリセットするリセット手段をさらに備える

ことを特徴とする請求項14に記載の情報処理装置。

【請求項23】 他の情報処理装置とネットワークを介して接続される情報処理装置の情報処理方法において、

前記他の情報処理装置との通信が確立したとき、前記情報処理装置の最初の位置を特定する第1の位置情報、および、前記他の情報処理装置の最初の位置を特定する第2の位置情報の記憶を制御する記憶制御ステップと、

前記情報処理装置の現在の位置を特定する第3の位置情報を取得する第1の取得ステップと、

前記第1の取得ステップの処理により取得された前記第3の位置情報が、前記記憶制御ステップの処理により記憶が制御されている前記第1の位置情報に対応するか否かを判定する第1の判定ステップと、

前記他の情報処理装置の現在の位置を特定する第4の位置情報を取得する第2の取得ステップと、

前記第2の取得ステップの処理により取得された前記第4の位置情報が、前記記憶制御ステップの処理により記憶が制御されている前記第2の位置情報に対応するか否かを判定する第2の判定ステップと、

前記第1および第2の判定ステップの処理による判定結果に基づいて、前記他の情報処理装置にデータを送信する送信ステップと

を含むことを特徴とする情報処理方法。

【請求項24】 他の情報処理装置とネットワークを介して接続される情報処理装置を制御するプログラムにおいて、

前記他の情報処理装置との通信が確立したとき、前記情報処理装置の最初の位置を特定する第1の位置情報、および、前記他の情報処理装置の最初の位置を特定する第2の位置情報の記憶を制御する記憶制御ステップと、



前記情報処理装置の現在の位置を特定する第 3 の位置情報を取得する第 1 の取得ステップと、

前記第 1 の取得ステップの処理により取得された前記第 3 の位置情報が、前記記憶制御ステップの処理により記憶が制御されている前記第 1 の位置情報に対応するか否かを判定する第 1 の判定ステップと、

前記他の情報処理装置の現在の位置を特定する第 4 の位置情報を取得する第 2 の取得ステップと、

前記第 2 の取得ステップの処理により取得された前記第 4 の位置情報が、前記記憶制御ステップの処理により記憶が制御されている前記第 2 の位置情報に対応するか否かを判定する第 2 の判定ステップと、

前記第 1 および第 2 の判定ステップの処理による判定結果に基づいて、前記他の情報処理装置にデータを送信する送信ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項 2 5】 他の情報処理装置とネットワークを介して接続されるコンピュータに、

前記他の情報処理装置との通信が確立したとき、前記情報処理装置の最初の位置を特定する第 1 の位置情報、および、前記他の情報処理装置の最初の位置を特定する第 2 の位置情報の記憶を制御する記憶制御ステップと、

前記情報処理装置の現在の位置を特定する第 3 の位置情報を取得する第 1 の取得ステップと、

前記第 1 の取得ステップの処理により取得された前記第 3 の位置情報が、前記記憶制御ステップの処理により記憶が制御されている前記第 1 の位置情報に対応するか否かを判定する第 1 の判定ステップと、

前記他の情報処理装置の現在の位置を特定する第 4 の位置情報を取得する第 2 の取得ステップと、

前記第 2 の取得ステップの処理により取得された前記第 4 の位置情報が、前記記憶制御ステップの処理により記憶が制御されている前記第 2 の位置情報に対応するか否かを判定する第 2 の判定ステップと、

前記第 1 および第 2 の判定ステップの処理による判定結果に基づいて、前記他の情報処理装置にデータを送信する送信ステップと  
を実行させることを特徴とするプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報処理装置および方法、記録媒体、並びにプログラムに関し、特に、既存のプロトコルを変更することなく、上位層での移動透過性を実現するようにした情報処理装置および方法、記録媒体、並びにプログラムに関する。

【0002】

【従来の技術】

近年、携帯型のパーソナルコンピュータの普及に伴い、ユーザは、パーソナルコンピュータを持ち運ぶことができるようになった。また、単に持ち運ぶだけでなく、その携帯型のパーソナルコンピュータを移動先のネットワークに接続し、ネットワークを介して様々なサービスを受けることができる。

【0003】

このような、いわゆるモバイルコンピューティング環境では、ネットワークに接続してサービスを受ける装置（パーソナルコンピュータ）であるノードは、移動することが前提となる。このようなノードは、ノードの位置が変化しても、継続して通信できるようにする必要がある。

【0004】

現在、IPv6（Internet Protocol version 6）の規格に基づいて、IPv6におけるネットワーク層での移動透過性を実現するためのプロトコルとして、IETF（the Internet Engineering Task Force）で提案されているMobile IPv6や、本出願人が、特許出願第 2 0 0 0 - 0 0 0 5 6 0 号として先に提案した手法（以下の手法をVIPv6と称する）などがある。

【0005】

【発明が解決しようとする課題】

上記した特許出願第 2 0 0 0 - 0 0 0 5 6 0 号で提案されている手法では、IP

v6アドレスの下位64ビットをユニークなものとして、IP層での移動透過を実現している。

【0006】

しかしながら、IPsec (Security Architecture for Internet Protocol) 層や上位層 (TCP/UDP (User Datagram Protocol)) でのセッションは、既存のプロトコルを変更しなければ、移動透過性を実現することができない課題があった。

【0007】

そこで、IPv6アドレスの上位64ビットであるネットワークプレフィックスに、所定の固定値を割り当てるようにする手法も考えられるが、上記した特許出願第2000-000560号におけるVIPv6のプロトコルに対して、特別な固定のネットワークプレフィックスを用いるという標準化が必要になる。

【0008】

すなわち、受信側のノードは、パケットを受信すると、IPsec層や上位層 (TCP/UDP) でセッションを行うのか、あるいは、受信パケットに含まれる送信元アドレスを用いて、通常のセッションを行うのかを判断する必要がある。そのためには、IPv6アドレスの下位64ビットにノードを識別するIDを記述するか、あるいは、ドメインネームサーバに“固定値+ノード識別ID”を示して、このアドレスが登録されているか否かの確認を行わなければならない。

【0009】

しかしながら、そのようにすると、少なくとも1つのネットワークプレフィックスが、IPsec層や上位層でのセッション専用に使われることになり、アドレスが無駄になる課題があった。

【0010】

本発明はこのような状況に鑑みてなされたものであり、既存のプロトコルを変更することなく、IPsec層およびトランスポート層での移動透過性を実現することができるようにするものである。

【0011】

【課題を解決するための手段】

本発明の第1の情報処理装置は、他の情報処理装置との通信が確立したとき、

情報処理装置の最初の位置を特定する第1の位置情報、および、他の情報処理装置の最初の位置を特定する第2の位置情報を記憶する記憶手段と、他の情報処理装置からデータを受信する受信手段と、情報処理装置の現在の位置を特定する第3の位置情報を取得する取得手段と、取得手段により取得された第3の位置情報が、記憶手段に記憶されている第1の位置情報に対応するか否かを判定する第1の判定手段と、第1の判定手段による判定結果に基づいて、受信手段により受信されたデータを認証する認証手段とを備えること特徴とする。

## 【0012】

前記第1の判定手段による判定の結果、第3の位置情報が第1の位置情報に対応しないと判定された場合、受信手段により受信されたデータに含まれる、送信先アドレスである情報処理装置の第4の位置情報、および、送信元アドレスである他の情報処理装置の第5の位置情報を読み取る読み取り手段と、読み取り手段により読み取られた第5の位置情報が、記憶手段に記憶されている第2の位置情報に対応するか否かを判定する第2の判定手段とをさらに設けるようにすることができる。

## 【0013】

前記第1の判定手段による判定の結果、第3の位置情報が第1の位置情報に対応しないと判定された場合、第4の位置情報を第1の位置情報により置換する置換手段をさらに設けるようにすることができる。

## 【0014】

前記第2の判定手段による判定の結果、第5の位置情報が第2の位置情報に対応しないと判定された場合、第5の位置情報を第2の位置情報により置換する置換手段をさらに設けるようにすることができる。

## 【0015】

前記第4の位置情報は、送信先アドレスの上位の一部のビットに割り当てられているようにすることができる。

## 【0016】

前記第5の位置情報は、送信元アドレスの上位の一部のビットに割り当てられているようにすることができる。

【0017】

前記認証手段は、受信手段により受信されたデータを認証するのに、さらに第1および第2の位置情報を用いるようにすることができる。

【0018】

前記情報処理装置が他のネットワークに接続されたとき、情報処理装置の現在の位置を特定する第4の位置情報および情報処理装置を特定する識別情報を、ネットワークに接続されている情報蓄積装置に通知する通知手段をさらに設けるようにすることができる。

【0019】

前記識別情報は、ネットワーク上において、情報処理装置を特定する端末識別子であるようにすることができる。

【0020】

前記他の情報処理装置との通信が切断されたとき、記憶手段に記憶されている第1および第2の位置情報をリセットするリセット手段をさらに設けるようにすることができる。

【0021】

本発明の第1の情報処理方法は、他の情報処理装置との通信が確立したとき、情報処理装置の最初の位置を特定する第1の位置情報、および、他の情報処理装置の最初の位置を特定する第2の位置情報の記憶を制御する記憶制御ステップと、他の情報処理装置からデータを受信する受信ステップと、情報処理装置の現在の位置を特定する第3の位置情報を取得する取得ステップと、取得ステップの処理により取得された第3の位置情報が、記憶制御ステップの処理により記憶が制御されている第1の位置情報に対応するか否かを判定する判定ステップと、第1の判定ステップの処理による判定結果に基づいて、受信ステップの処理により受信されたデータを認証する認証ステップとを含むことを特徴とする。

【0022】

本発明の第1の記録媒体に記録されているプログラムは、他の情報処理装置との通信が確立したとき、情報処理装置の最初の位置を特定する第1の位置情報、および、他の情報処理装置の最初の位置を特定する第2の位置情報の記憶を制御

する記憶制御ステップと、他の情報処理装置からデータを受信する受信ステップと、情報処理装置の現在の位置を特定する第3の位置情報を取得する取得ステップと、取得ステップの処理により取得された第3の位置情報が、記憶制御ステップの処理により記憶が制御されている第1の位置情報に対応するか否かを判定する判定ステップと、第1の判定ステップの処理による判定結果に基づいて、受信ステップの処理により受信されたデータを認証する認証ステップとを含むことを特徴とする。

## 【0023】

本発明の第1のプログラムは、他の情報処理装置との通信が確立したとき、情報処理装置の最初の位置を特定する第1の位置情報、および、他の情報処理装置の最初の位置を特定する第2の位置情報の記憶を制御する記憶制御ステップと、他の情報処理装置からデータを受信する受信ステップと、情報処理装置の現在の位置を特定する第3の位置情報を取得する取得ステップと、取得ステップの処理により取得された第3の位置情報が、記憶制御ステップの処理により記憶が制御されている第1の位置情報に対応するか否かを判定する判定ステップと、第1の判定ステップの処理による判定結果に基づいて、受信ステップの処理により受信されたデータを認証する認証ステップとをコンピュータに実行させることを特徴とする。

## 【0024】

本発明の第1の情報処理装置および方法、並びにプログラムにおいては、他の情報処理装置との通信が確立したとき、情報処理装置の最初の位置を特定する第1の位置情報、および、他の情報処理装置の最初の位置を特定する第2の位置情報が記憶され、他の情報処理装置からデータが受信され、情報処理装置の現在の位置を特定する第3の位置情報が取得され、取得された第3の位置情報が第1の位置情報に対応するか否かが判定され、その判定結果に基づいて、受信されたデータが認証される。

## 【0025】

本発明の第2の情報処理装置は、他の情報処理装置との通信が確立したとき、情報処理装置の最初の位置を特定する第1の位置情報、および、他の情報処理装

置の最初の位置を特定する第2の位置情報を記憶する記憶手段と、情報処理装置の現在の位置を特定する第3の位置情報を取得する第1の取得手段と、第1の取得手段により取得された第3の位置情報が、記憶手段に記憶されている第1の位置情報に対応するか否かを判定する第1の判定手段と、他の情報処理装置の現在の位置を特定する第4の位置情報を取得する第2の取得手段と、第2の取得手段により取得された第4の位置情報が、記憶手段に記憶されている第2の位置情報に対応するか否かを判定する第2の判定手段と、第1および第2の判定手段の判定結果に基づいて、他の情報処理装置にデータを送信する送信手段とを備えることを特徴とする。

## 【0026】

前記第1の判定手段による判定の結果、第3の位置情報が第1の位置情報に対応しないと判定された場合、第3の位置情報を第1の位置情報により置換する置換手段をさらに設けるようにすることができる。

## 【0027】

前記第2の判定手段による判定の結果、第4の位置情報が第2の位置情報に対応しないと判定された場合、第4の位置情報を第2の位置情報により置換する置換手段をさらに設けるようにすることができる。

## 【0028】

前記記憶手段に記憶されている第1および第2の位置情報を用いて、データに付加する付加情報を演算する演算手段と、演算手段により演算された付加情報をデータに付加する付加手段とをさらに設けるようにすることができ、前記送信手段は、第1の取得手段により取得された第3の位置情報を送信元アドレスに設定するとともに、第2の取得手段により取得された第4の位置情報を送信先アドレスに設定して、付加手段により付加情報が付加されたデータを送信することができる。

## 【0029】

前記第3の位置情報は、送信先アドレスの上位の一部のビットに割り当てられているようにすることができる。

## 【0030】

前記第 4 の位置情報は、送信元アドレスの上位の一部のビットに割り当てられているようにすることができる。

【 0 0 3 1 】

前記情報処理装置が他のネットワークに接続されたとき、情報処理装置の現在の位置を特定する第 5 の位置情報および情報処置装置を特定する識別情報を、ネットワークに接続されている情報蓄積装置に通知する通知手段をさらに設けるようにすることができる。

【 0 0 3 2 】

前記識別情報は、ネットワーク上において、情報処理装置を特定する端末識別子であるようにすることができる。

【 0 0 3 3 】

前記他の情報処理装置との通信が切断されたとき、記憶手段に記憶されている第 1 および第 2 の位置情報をリセットするリセット手段をさらに設けるようにすることができる。

【 0 0 3 4 】

本発明の第 2 の情報処理方法は、他の情報処理装置との通信が確立したとき、情報処理装置の最初の位置を特定する第 1 の位置情報、および、他の情報処置装置の最初の位置を特定する第 2 の位置情報の記憶を制御する記憶制御ステップと、情報処理装置の現在の位置を特定する第 3 の位置情報を取得する第 1 の取得ステップと、第 1 の取得ステップの処理により取得された第 3 の位置情報が、記憶制御ステップの処理により記憶が制御されている第 1 の位置情報に対応するか否かを判定する第 1 の判定ステップと、他の情報処理装置の現在の位置を特定する第 4 の位置情報を取得する第 2 の取得ステップと、第 2 の取得ステップの処理により取得された第 4 の位置情報が、記憶制御ステップの処理により記憶が制御されている第 2 の位置情報に対応するか否かを判定する第 2 の判定ステップと、第 1 および第 2 の判定ステップの処理による判定結果に基づいて、他の情報処理装置にデータを送信する送信ステップとを含むことを特徴とする。

【 0 0 3 5 】

本発明の第 2 の記録媒体に記録されているプログラムは、他の情報処理装置と



の通信が確立したとき、情報処理装置の最初の位置を特定する第1の位置情報、および、他の情報処理装置の最初の位置を特定する第2の位置情報の記憶を制御する記憶制御ステップと、情報処理装置の現在の位置を特定する第3の位置情報を取得する第1の取得ステップと、第1の取得ステップの処理により取得された第3の位置情報が、記憶制御ステップの処理により記憶が制御されている第1の位置情報に対応するか否かを判定する第1の判定ステップと、他の情報処理装置の現在の位置を特定する第4の位置情報を取得する第2の取得ステップと、第2の取得ステップの処理により取得された第4の位置情報が、記憶制御ステップの処理により記憶が制御されている第2の位置情報に対応するか否かを判定する第2の判定ステップと、第1および第2の判定ステップの処理による判定結果に基づいて、他の情報処理装置にデータを送信する送信ステップとを含むことを特徴とする。

## 【 0 0 3 6 】

本発明の第2のプログラムは、他の情報処理装置との通信が確立したとき、情報処理装置の最初の位置を特定する第1の位置情報、および、他の情報処理装置の最初の位置を特定する第2の位置情報の記憶を制御する記憶制御ステップと、情報処理装置の現在の位置を特定する第3の位置情報を取得する第1の取得ステップと、第1の取得ステップの処理により取得された第3の位置情報が、記憶制御ステップの処理により記憶が制御されている第1の位置情報に対応するか否かを判定する第1の判定ステップと、他の情報処理装置の現在の位置を特定する第4の位置情報を取得する第2の取得ステップと、第2の取得ステップの処理により取得された第4の位置情報が、記憶制御ステップの処理により記憶が制御されている第2の位置情報に対応するか否かを判定する第2の判定ステップと、第1および第2の判定ステップの処理による判定結果に基づいて、他の情報処理装置にデータを送信する送信ステップとをコンピュータに実行させることを特徴とする。

## 【 0 0 3 7 】

本発明の第2の情報処理装置および方法、並びにプログラムにおいては、他の情報処理装置との通信が確立したとき、情報処理装置の最初の位置を特定する第

1 の位置情報、および、他の情報処理装置の最初の位置を特定する第 2 の位置情報が記憶され、情報処理装置の現在の位置を特定する第 3 の位置情報が取得され、取得された第 3 の位置情報が第 1 の位置情報に対応するか否かが判定され、他の情報処理装置の現在の位置を特定する第 4 の位置情報が取得され、取得された第 4 の位置情報が第 2 の位置情報に対応するか否かが判定され、それらの判定結果に基づいて、他の情報処理装置にデータが送信される。

【 0 0 3 8 】

【発明の実施の形態】

図 1 は、本発明のネットワークシステムの一実施の形態の構成を示す図である。同図に示されるネットワークシステムにおいて、ネットワークを構成する端末装置 1 および端末装置 3 などのノードは、IPv6 アドレスを基に、通信を実行する。

【 0 0 3 9 】

IPv6 アドレスは、図 2 に示されるように、128 ビットからなり、IPv6 アドレスの上位 64 ビットは、ネットワークプレフィックス (Network Prefix) と称され、下位 64 ビットは、端末識別子 (Interface ID) と称される。

【 0 0 4 0 】

ネットワークプレフィックスは、3 ビットの FP (Format Prefix)、13 ビットの TLA ID (Top Level Aggregation Identifier)、8 ビットの rsvd (Reserved)、24 ビットの NLA ID (Next Level Aggregation Identifier)、および、16 ビットの SLA ID (Site Level Aggregation Identifier) から構成されている。ネットワークプレフィックスのうちの、FP、TLA ID、rsvd、および、NLA ID は、パブリックトポロジと称され、SLA ID は、サイトトポロジと称される。

【 0 0 4 1 】

ネットワークプレフィックスは、ノードが接続されているサブネットワーク（例えば、図 1 におけるサブネットワーク 9-1 乃至 9-7 および無線サブネットワーク 7-1 乃至 7-4 のいずれか）を示しており、そのノードにパケットを送信するために利用される。

【 0 0 4 2 】

端末識別子は、インターネット 5 上で端末装置 1 や端末装置 3 などのノード自体を一意に識別するための識別子を示しており、ノードの位置または移動によりその値が変化することはない。これはノードの認識または認証に利用される。

【0043】

図 3 は、本発明の IPv6 におけるプロトコル層の構成例を示す図である。IPv6 におけるプロトコル層は、アプリケーション層、TCP/UDP 層、IPsec 層、IP 層、データリンク層、および、物理層から構成される。

【0044】

図 1 の説明に戻る。携帯型で、移動自在な端末装置 1 は、基地局 6-1 の無線サブネットワーク 7-1 内に位置するとき、無線により、基地局 6-1 と通信して、ルータ 8-5、サブネットワーク 9-4、ルータ 8-3、サブネットワーク 9-2、ルータ 8-2、サブネットワーク 9-1、およびルータ 8-1 を介して、インターネット 5 に接続する。

【0045】

端末装置 1 は、基地局 6-2 の無線サブネットワーク 7-2 内に位置するとき、無線により、基地局 6-2 と通信して、ルータ 8-6、サブネットワーク 9-5、ルータ 8-3、サブネットワーク 9-2、ルータ 8-2、サブネットワーク 9-1、およびルータ 8-1 を介して、インターネット 5 に接続する。

【0046】

端末装置 1 は、基地局 6-3 の無線サブネットワーク 7-3 内に位置するとき、無線により、基地局 6-3 と通信して、ルータ 8-7、サブネットワーク 9-6、ルータ 8-4、サブネットワーク 9-3、ルータ 8-2、サブネットワーク 9-1、およびルータ 8-1 を介して、インターネット 5 に接続する。

【0047】

端末装置 1 は、基地局 6-4 の無線サブネットワーク 7-4 内に位置するとき、無線により、基地局 6-4 と通信して、ルータ 8-8、サブネットワーク 9-7、ルータ 8-4、サブネットワーク 9-3、ルータ 8-2、サブネットワーク 9-1、およびルータ 8-1 を介して、インターネット 5 に接続する。

【0048】

ホームエージェント2-1は、端末装置1の端末識別子とネットワークプレフィックスとの対応を記憶している。ホームエージェント2-2も、端末装置1の端末識別子とネットワークプレフィックスとの対応を記憶している。

【0049】

端末装置3は、インターネット5に接続され、インターネット5等を介して、端末装置1と通信する。

【0050】

ドメインネームサーバ4は、各端末装置のホスト名に対応して、各端末装置の端末識別子、および、各端末装置に関係付けられたマッピングエージェント（図6を参照して後述する）のIPv6アドレスを記憶する。

【0051】

基地局6-1は、無線サブネットワーク7-1を形成し、無線により、無線サブネットワーク7-1内に位置する端末装置1と通信し、端末装置1が送信するパケットを受信して、受信したパケットをルータ8-5に供給するとともに、ルータ8-5から入力された端末装置1宛てのパケットを端末装置1に送信する。

【0052】

基地局6-1は、無線サブネットワーク7-1内に位置する端末装置1に、無線サブネットワーク7-1に対応するネットワークプレフィックスを供給する。

【0053】

基地局6-2は、無線サブネットワーク7-2を形成し、無線により、無線サブネットワーク7-2内に位置する端末装置1と通信し、端末装置1が送信するパケットを受信して、受信したパケットをルータ8-6に供給するとともに、ルータ8-6から入力された端末装置1宛てのパケットを端末装置1に送信する。

【0054】

基地局6-2は、無線サブネットワーク7-2内に位置する端末装置1に、無線サブネットワーク7-2に対応するネットワークプレフィックスを供給する。

【0055】

基地局6-3は、無線サブネットワーク7-3を形成し、無線により、無線サブネットワーク7-3内に位置する端末装置1と通信し、端末装置1が送信する

パケットを受信して、受信したパケットをルータ8-7に供給するとともに、ルータ8-7から入力された端末装置1宛てのパケットを端末装置1に送信する。

【0056】

基地局6-3は、無線サブネットワーク7-3内に位置する端末装置1に、無線サブネットワーク7-3に対応するネットワークプレフィックスを供給する。

【0057】

基地局6-4は、無線サブネットワーク7-4を形成し、無線により、無線サブネットワーク7-4内に位置する端末装置1と通信し、端末装置1が送信するパケットを受信して、受信したパケットをルータ8-8に供給するとともに、ルータ8-8から入力された端末装置1宛てのパケットを端末装置1に送信する。

【0058】

基地局6-4は、無線サブネットワーク7-4内に位置する端末装置1に、無線サブネットワーク7-4に対応するネットワークプレフィックスを供給する。

【0059】

基地局6-1乃至6-4は、複数の端末装置と通信するので、無線サブネットワーク7-1乃至7-4は、無線によるサブネットワークを形成する。

【0060】

ルータ8-1乃至8-8は、それぞれ、端末識別子に対応させてネットワークプレフィックスなどを記憶して、端末装置1、端末装置3、ホームエージェント2-1もしくは2-2、またはドメインネームサーバ4から供給されたパケットが送信される経路を制御（ルーティング）する。

【0061】

以下、ホームエージェント2-1および2-2を個々に区別する必要がないとき、単にホームエージェント2と称する。基地局6-1乃至6-4を個々に区別する必要がないとき、単に基地局6と称する。無線サブネットワーク7-1乃至7-4を個々に区別する必要がないとき、単に無線サブネットワーク7と称する。ルータ8-1乃至8-8を個々に区別する必要がないとき、単にルータ8と称する。サブネットワーク9-1乃至9-7を個々に区別する必要がないとき、単にサブネットワーク9と称する。

【 0 0 6 2 】

図 4 は、端末装置 1 の構成例を示すブロック図である。

【 0 0 6 3 】

CPU (Central Processing Unit) 2 1 は、各種アプリケーションプログラムや、OS (Operating System)を実際に実行する。ROM (Read-only Memory) 2 2 は、一般的には、CPU 2 1 が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。RAM (Random-Access Memory) 2 3 は、CPU 2 1 の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。これらはCPUバスなどから構成されるホストバス 2 4 により相互に接続されている。

【 0 0 6 4 】

ホストバス 2 4 は、ブリッジ 2 5 を介して、PCI (Peripheral Component Interconnect/Interface) バスなどの外部バス 2 6 に接続されている。

【 0 0 6 5 】

キーボード 2 8 は、CPU 2 1 に各種の指令を入力するとき、使用者により操作される。ポインティングデバイス 2 9 は、ディスプレイ 3 0 の画面上のポイントの指示や選択を行うとき、使用者により操作される。ディスプレイ 3 0 は、液晶表示装置などからなり、各種情報をテキストやイメージで表示する。ハードディスクドライブ (HD: Hard Disk Drive) 3 1 は、ハードディスクを駆動し、それらにCPU 2 1 によって実行するプログラムや情報を記録または再生させる。

【 0 0 6 6 】

ドライブ 3 2 は、装着されている磁気ディスク 4 1、光ディスク 4 2、光磁気ディスク 4 3、または半導体メモリ 4 4 に記録されているデータまたはプログラム (通信部 3 3 が実行するプログラムを含む) を読み出して、そのデータまたはプログラムを、インターフェース 2 7、外部バス 2 6、ブリッジ 2 5、およびホストバス 2 4 を介して接続されているRAM 2 3 または通信部 3 3 に供給する。これらのキーボード 2 8 乃至ドライブ 3 2 は、インターフェース 2 7 に接続されており、インターフェース 2 7 は、外部バス 2 6、ブリッジ 2 5、およびホストバス 2 4 を介してCPU 2 1 に接続されている。

【0067】

通信部33は、基地局6と通信し、CPU21、またはハードディスクドライブ31から供給されたデータを、所定の方式のパケットに格納して、基地局6に送信するとともに、基地局6から受信したパケットに格納されているデータをCPU21、RAM23、またはハードディスクドライブ31に出力する。

【0068】

通信部33は、外部バス26、ブリッジ25、およびホストバス24を介してCPU21に接続されている。

【0069】

ホームエージェント2-1および2-2、端末装置3、並びにドメインネームサーバ4は、端末装置1と同様の構成を有するので、その説明は省略する。

【0070】

図5は、ルータ8-1の構成例を示すブロック図である。

【0071】

CPU51は、所定のプログラムを実際に実行する。ROM52は、一般的には、CPU51が実行するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。RAM53は、CPU51の実行において実行するプログラムや、その実行において適宜変化するパラメータを格納する。

【0072】

ドライブ55は、装着されている磁気ディスク61、光ディスク62、光磁気ディスク63、または半導体メモリ64に記録されているデータまたはプログラム（通信部56または通信部57が実行するプログラムを含む）を読み出して、そのデータまたはプログラムを、バス54を介して接続されているRAM53、通信部56、または通信部57に供給する。

【0073】

通信部56は、インターネット5が接続され、CPU51または通信部57から供給されたデータを、所定の方式のパケットに格納して、インターネット5を介して、送信するとともに、インターネット5を介して、受信したパケットに格納されているデータをCPU51または通信部57に出力する。

## 【0074】

通信部57は、サブネットワーク9-1が接続され、CPU51または通信部56から供給されたデータを、所定の方式のパケットに格納して、サブネットワーク9-1を介して、送信するとともに、サブネットワーク9-1を介して、受信したパケットに格納されているデータをCPU51または通信部56に出力する。

## 【0075】

これらのCPU51乃至通信部57は、バス54により相互に接続されている。

## 【0076】

ルータ8-2乃至8-8の構成は、ルータ8-1と同様であるので、その説明は省略する。

## 【0077】

次に、本発明の実施の形態における、端末装置1と端末装置3との間のパケットデータのルーティング通信の動作について、図6を参照して説明する。

## 【0078】

端末装置3は、ドメインネームサーバ4に端末装置1のホスト名を示して、端末装置1の端末識別子、および、端末装置1に関係付けられたマッピングエージェント81（その詳細は後述する）のIPv6アドレス（図2）を問い合わせる。ドメインネームサーバ4は、ホスト名に対応して、端末装置1の端末識別子および端末装置1に関係付けられたマッピングエージェント81のIPv6アドレスを記憶しているので、端末装置1の端末識別子および端末装置1に関係付けられたマッピングエージェント81のIPv6アドレスを読み出して、読み出した端末識別子およびマッピングエージェント81のIPv6アドレスを端末装置3に送信する。

## 【0079】

端末装置3は、ドメインネームサーバ4から受信した1以上のマッピングエージェント81に対応するIPv6アドレスから1つのIPv6アドレスを選択して、選択したIPv6アドレスを基に、マッピングエージェント81に、端末装置1の端末識別子を示して、端末装置1の現在のネットワークプレフィックスを問い合わせる。

## 【0080】



マッピングエージェント 81 は、任意のサブネットワークに接続され、端末装置 1 の端末識別子に対応して、端末装置 1 の現在のネットワークプレフィックスを記憶する。従って、マッピングエージェント 81 は、問い合わせのあった端末装置 3 に、端末装置 1 の現在のネットワークプレフィックスを送信する。端末装置 3 は、マッピングエージェント 81 から受信した端末装置 1 の現在のネットワークプレフィックスをバインディングキャッシュ (binding cache) に登録または更新 (アップデート) する。

## 【0081】

端末装置 3 は、端末装置 1 の現在のネットワークプレフィックスと端末識別子を結合して IPv6 アドレスを生成し、さらに、生成した IPv6 アドレスをデータパケットの送信先アドレスに設定し、そのデータパケットを端末装置 1 に送信する。

## 【0082】

端末装置 3 が端末装置 1 に送信したデータパケットは、送信先の IPv6 アドレスに、端末装置 1 の現在のネットワークプレフィックスと端末識別子が設定されているので、最適な経路を通過して、端末装置 1 に到達することができる。

## 【0083】

端末装置 1 に対応するマッピングエージェント 81 は、1 以上とされる。従って、端末装置 3 は、1 つのマッピングエージェント 81 が故障しても、他のマッピングエージェント 81 を利用することができるので、端末装置 1 との通信を実行することができる。

## 【0084】

端末装置 1 が端末装置 3 に送信したデータパケットは、端末装置 1 の現在のネットワークプレフィックスと端末識別子が、その送信元に設定され、端末装置 3 の IPv6 アドレスが、その送信先に設定されているので、最適な経路を通過して、端末装置 3 に到達する。

## 【0085】

また、端末装置 1 が移動した場合、端末装置 1 は、Router Solicitation にて、ルータ 8 に問い合わせることにより、Router Advertisement を要求し、取得する。ルータ 8 から提供される Router Advertisement には、新たに移動して接続し

たネットワークのネットワークプレフィックスが含まれている。そして、端末装置1は、認証ヘッダ（図7）、および送信元アドレスに、取得した端末装置1の現在のネットワークプレフィックスを含んだbinding updateパケットを生成して、マッピングエージェント81に送信することで、端末装置1の現在のネットワークプレフィックスをマッピングエージェント81に通知する。

## 【0086】

認証ヘッダは、図7に示されるように、4バイトで構成されており、SPI（Security Parameters Index）、シーケンスナンバー、および、認証データ等を含んでいる。

## 【0087】

マッピングエージェント81は、端末装置1よりbinding updateパケットを受信すると、送信元のアドレスの端末識別子および認証ヘッダのSPIを基にSA（Security Association）を判別して、認証用の鍵、または暗号化方式等を決定して、認証処理を実行する。認証データが正しいと判定された場合、マッピングエージェント81は、binding updateパケットに格納されている端末装置1の現在のネットワークプレフィックスをbinding cacheに登録または更新（アップデート）する。

## 【0088】

次に、図8のフローチャートを参照して、端末装置1と端末装置3との間で、図6に示したようなパケットデータのルーティング通信が開始されたときに行われる初期設定処理について説明する。

## 【0089】

ステップS1において、端末装置1のCPU21は、端末装置3との接続が完了したか否かを判定し、未だ端末装置3との接続が完了していないと判定した場合、接続処理を繰り返す。そして、端末装置1と端末装置3との間で接続が完了したと判定された場合、ステップS2に進み、端末装置1のCPU21は、ユーザによりキーボード28またはポインティングデバイス29が操作され、送信開始または受信開始に関するコマンドが入力されることにより、アプリケーション層から送信開始または受信開始が要求されたか否かを判定する。

## 【0090】

ステップS2において、未だ、送信開始または受信開始が要求されていないと判定された場合、送信開始または受信開始が要求されるまで待機し、送信開始または受信開始が要求されると、ステップS3に進む。

## 【0091】

ステップS3において、端末装置1のCPU21は、端末装置1の最初のネットワークプレフィックス（すなわち、端末装置1のIPv6アドレスの上位64ビット）、および、マッピングエージェント81より取得した接続相手である端末装置3の最初のネットワークプレフィックス（すなわち、端末装置3のIPv6アドレスの上位64ビット）を、ハードディスクドライブ31に記憶させる。

## 【0092】

ステップS4において、端末装置3のCPU21は、端末装置1と同様に、端末装置3の最初のネットワークプレフィックス（すなわち、端末装置3のIPv6アドレスの上位64ビット）、および、マッピングエージェント81より取得した接続相手である端末装置1の最初のネットワークプレフィックス（すなわち、端末装置1のIPv6アドレスの上位64ビット）を、ハードディスクドライブ（HDD）31に記憶させる。

## 【0093】

端末装置1と端末装置3との間で通信が継続する限り、端末装置1または端末装置3のいずれか一方、もしくは、両方が移動した場合にも、以上の初期設定処理により、最初に接続されたときに記憶されたネットワークプレフィックスが、IPsecの認証時において、認証データの演算およびチェックサムの演算に利用される。

## 【0094】

なお、通信が切断された場合、ハードディスクドライブ31およびハードディスクドライブ31に記憶されているネットワークプレフィックスは、全てクリアされる。

## 【0095】

次に、図9のフローチャートを参照して、端末装置1の移動時の通信処理につ

いて説明する。

【0096】

ステップS11において、端末装置1のCPU21は、移動先の無線サブネットワーク7から、Router Solicitationにて、ルータ8に問い合わせることにより、Router Advertisementを要求する。ステップS12において、端末装置1のCPU21は、ルータ8から提供されるRouter Advertisementを受け取り、その中に含まれる、新たに移動して接続したネットワークのネットワークプレフィックスを取得する。

【0097】

ステップS13において、端末装置1のCPU21は、ステップS12の処理で取得されたネットワークのネットワークプレフィックスが、図8の初期設定処理でハードディスクドライブ31に記憶されている端末装置1の最初のネットワークプレフィックスと同じであるか否かを判定する。

【0098】

ステップS13において、ステップS12の処理で取得されたネットワークプレフィックスが、ハードディスクドライブ31に記憶されている端末装置1の最初のネットワークプレフィックスと同じではないと判定された場合、ステップS14に進み、端末装置1のCPU21は、ステップS12の処理で取得されたネットワークプレフィックスと、自分の端末識別子を対応させる。これにより、端末装置1の端末識別子と、現在接続されているネットワークのネットワークプレフィックスのマッピング参照情報が得られる。

【0099】

ステップS15において、端末装置1のCPU21は、マッピング参照情報を含んだbinding updateパケットを生成して、マッピングエージェント81に送信する。ステップS16において、マッピングエージェント81は、端末装置1よりbinding updateパケットを受信すると、送信先のアドレスの端末識別子および認証ヘッダのSPIを基にSAを判別して、認証用の鍵、または暗号化方式等を決定して、認証処理を実行する。認証データが正しいと判定された場合、マッピングエージェント81は、binding updateパケットに含まれるマッピング参照情報に基

づいて、binding cacheを更新する。これにより、端末装置1の端末識別子に対応して、端末装置1の現在のネットワークプレフィックスがマッピングエージェント81のbinding cacheに記憶される。

#### 【0100】

ステップS13において、ステップS12の処理で取得されたネットワークプレフィックスが、ハードディスクドライブ31に記憶されている端末装置1の最初のネットワークプレフィックスと同じであると判定された場合、それ以降のステップS14乃至S16の処理は実行されずに、処理は終了される。

#### 【0101】

このように、端末装置1が移動したとき、新たに移動して接続したネットワークのネットワークプレフィックスと、記憶されている最初のネットワークプレフィックスが同じでない場合にのみ、情報の更新を行うようにしたので、より効率的に通信経路を確立することができる。

#### 【0102】

また、端末装置3は、接続相手である端末装置1が移動したことを何等かの方法により知ると、マッピングエージェント81に、再度、端末装置1の端末識別子を示して、端末装置1の現在のネットワークプレフィックスを問い合わせる。問い合わせを受けたマッピングエージェント81は、端末装置1の端末識別子に対応して記憶されている、端末装置1の現在のネットワークプレフィックスを端末装置3に送信する。これにより、端末装置3は、マッピングエージェント81から受信した端末装置1の現在のネットワークプレフィックスをbinding cacheに更新する。そして、端末装置3は、端末装置1の現在のネットワークプレフィックスと端末識別子を結合してIPv6アドレスを生成し、さらに、生成したIPv6アドレスを送信先に設定したデータパケットを端末装置1に送信する。

#### 【0103】

次に、図10のフローチャートを参照して、端末装置1の受信処理について説明する。

#### 【0104】

ステップS31において、端末装置1のCPU21は、アプリケーション層での

通信が再開されたか否かを判定し、アプリケーション層での通信が再開されるまで待機する。そして、アプリケーション層での通信が再開されたと判定された場合、端末装置 3 より送信されてくるデータパケットを受信した後、ステップ S 3 2 に進み、端末装置 1 の CPU 2 1 は、Router Solicitation にて、ルータ 8 に問い合わせることにより、Router Advertisement を要求する。

## 【 0 1 0 5 】

ステップ S 3 3 において、端末装置 1 の CPU 2 1 は、ルータ 8 から提供される Router Advertisement を受け取り、その中に含まれる、自分が現在接続しているネットワークのネットワークプレフィックスを取得する。ステップ S 3 4 において、端末装置 1 の CPU 2 1 は、ステップ S 3 3 の処理で取得されたネットワークのネットワークプレフィックスが、図 8 の初期設定処理でハードディスクドライブ 3 1 に記憶されている端末装置 1 の最初のネットワークプレフィックスと同じであるか否かを判定する。

## 【 0 1 0 6 】

ステップ S 3 4 において、ステップ S 3 3 の処理で取得されたネットワークプレフィックスが、ハードディスクドライブ 3 1 に記憶されている端末装置 1 の最初のネットワークプレフィックスと同じではないと判定された場合、ステップ S 3 5 に進み、上述した移動時の通信処理（図 9）を実行した後、ステップ S 3 6 に進む。

## 【 0 1 0 7 】

ステップ S 3 6 において、端末装置 1 の CPU 2 1 は、端末装置 3 からの受信パケットの送信先アドレス（DESTINATION IP ADDRESS）の上位 6 4 ビットである destination address（すなわち、端末装置 1 の IPv6 アドレスのネットワークプレフィックス）を読み取る。

## 【 0 1 0 8 】

ステップ S 3 7 において、端末装置 1 の CPU 2 1 は、送信先アドレスの上位 6 4 ビットの destination address を、ハードディスクドライブ 3 1 に記憶されている端末装置 1 の最初のネットワークプレフィックスに置換する。すなわち、送信先アドレスの上位 6 4 ビットの destination address には、端末装置 1 の最初

のネットワークプレフィックスが記述される。

【0109】

ステップS34において、ステップS33の処理で取得されたネットワークプレフィックスが、ハードディスクドライブ31に記憶されている端末装置1の最初のネットワークプレフィックスと同じであると判定された場合、ステップS35乃至S37の処理はスキップされる。

【0110】

ステップS38において、端末装置1のCPU21は、受信パケットの送信元アドレス (SOURCE IP ADDRESS) の上位64ビットであるsource address (すなわち、端末装置3のIPv6アドレスのネットワークプレフィックス) を読み取る。ステップS39において、端末装置1のCPU21は、ステップS38の処理で読み取られた送信元アドレスの上位64ビットのネットワークプレフィックスが、図8の初期設定処理でハードディスクドライブ31に記憶されている端末装置3の最初のネットワークプレフィックスと同じであるか否かを判定する。

【0111】

ステップS39において、ステップS38の処理で読み取られた送信元アドレスの上位64ビットのネットワークプレフィックスが、ハードディスクドライブ31に記憶されている端末装置3の最初のネットワークプレフィックスと同じではないと判定された場合、ステップS40に進み、端末装置1のCPU21は、送信元アドレスの上位64ビットのsource addressを、ハードディスクドライブ31に記憶されている端末装置3の最初のネットワークプレフィックスに置換する。すなわち、送信元アドレスの上位64ビットのsource addressには、端末装置3の最初のネットワークプレフィックスが記述される。

【0112】

ステップS39において、ステップS38の処理で読み取られた送信元アドレスの上位64ビットのネットワークプレフィックスが、ハードディスクドライブ31に記憶されている端末装置3の最初のネットワークプレフィックスと同じであると判定された場合、ステップS40の処理はスキップされる。

【0113】

ステップ S 4 1 において、端末装置 1 の CPU 2 1 は、図 1 1 に示されるような擬似ヘッダを生成する。

【 0 1 1 4 】

図 1 1 に示す擬似ヘッダにおいて、上述した処理により、SOURCE IP ADDRESS の上位 6 4 ビットの source address には、送信元である端末装置 3 の最初のネットワークプレフィックスが記述され、下位 6 4 ビットには、送信元の端末装置 3 を識別する端末識別子が記述される。また、DESTINATION IP ADDRESS の上位 6 4 ビットの destination address には、送信先である端末装置 1 の最初のネットワークプレフィックスが記述され、下位 6 4 ビットには、送信先の端末装置 1 を識別する端末識別子が記述される。ZERO には、単に “ 0 ” が定義され、PORT には、アプリケーションを指定するポート番号が定義され、TCP/UDP LENGTH には、TCP/UDP の長さ（チェックサム）が定義される。

【 0 1 1 5 】

ステップ S 4 2 において、端末装置 1 の CPU 2 1 は、ステップ S 4 1 の処理で生成された擬似ヘッダ（図 1 1）を用いて、受信パケットの認証データを演算する。認証データは、例えば、擬似ヘッダを含む受信パケットのハッシュ値を演算することにより得られる。そして、端末装置 1 は、演算された認証データと、受信パケットの認証ヘッダに含まれる認証データとを比較し、両者が対応すれば、通信相手は正当であるとして以後の処理を実行し、両者が対応しなければ、通信相手は正当な者ではないとして処理を終了させる。

【 0 1 1 6 】

認証データが照合されると、ステップ S 4 3 において、端末装置 1 の CPU 2 1 は、擬似ヘッダ（図 1 1）を用いて、TCP/UDP のチェックサムを演算し、受信パケットに誤りがあるか否かの照合を行う。誤りがあれば、その受信パケットは破棄される。誤りがなければ、その受信パケットの内容が取り込まれる。

【 0 1 1 7 】

ステップ S 4 4 において、端末装置 1 の CPU 2 1 は、アプリケーション層での通信が終了したか否かを判定し、アプリケーション層での通信が終了していないと判定した場合、ステップ S 3 2 に戻り、上述したそれ以降の処理を繰り返す。



そして、ステップS44において、アプリケーション層での通信が終了したと判定された場合、処理は終了される。

【0118】

このように、データパケットの受信時において、IP層の上位層に特別な変更を加えることなく、IPsec層およびトランスポート層（TCP/UDP）の移動透過性を保つことが可能となる。

【0119】

次に、図12のフローチャートを参照して、端末装置1の送信処理について説明する。

【0120】

ステップS61において、端末装置1のCPU21は、アプリケーション層での通信が再開されたか否かを判定し、アプリケーション層での通信が再開されるまで待機する。そして、アプリケーション層での通信が再開されたと判定されると、ステップS62に進み、端末装置1のCPU21は、Router Solicitationにて、ルータ8に問い合わせることにより、Router Advertisementを要求する。そして、端末装置1は、ルータ8から提供されるRouter Advertisementを受け取り、自分が現在接続しているネットワークのネットワークプレフィックスを取得する。

【0121】

ステップS63において、端末装置1のCPU21は、ステップS62の処理で取得されたネットワークプレフィックスが、図8の初期設定処理でハードディスクドライブ31に記憶されている端末装置1の最初のネットワークプレフィックスと同じであるか否かを判定する。

【0122】

ステップS63において、ステップS62の処理で取得されたネットワークプレフィックスが、ハードディスクドライブ31に記憶されている端末装置1の最初のネットワークプレフィックスと同じではないと判定された場合、ステップS64に進み、上述した移動時の通信処理（図9）を実行した後、ステップS65に進む。

【0123】

ステップS 6 5において、端末装置1のCPU 2 1は、送信パケットの送信元アドレス（SOURCE IP ADDRESS）の上位6 4ビットであるsource addressを、端末装置1の最初のネットワークプレフィックスに置換する。すなわち、送信元アドレスの上位6 4ビットのsource addressには、端末装置1の最初のネットワークプレフィックスが記述される。

## 【0 1 2 4】

ステップS 6 3において、ステップS 6 2の処理で取得されたネットワークプレフィックスが、ハードディスクドライブ3 1に記憶されている端末装置1の最初のネットワークプレフィックスと同じであると判定された場合、ステップS 6 4およびS 6 5の処理はスキップされる。

## 【0 1 2 5】

ステップS 6 6において、端末装置1のCPU 2 1は、端末装置3の現在のネットワークプレフィックスを取得する。

## 【0 1 2 6】

具体的には、端末装置1が、ドメインネームサーバ4に端末装置3のホスト名を示して、端末装置3の端末識別子、および、端末装置3に関係付けられたマッピングエージェント（図示せず）のIPv6アドレスを問い合わせる。ドメインネームサーバ4は、ホスト名に対応して、端末装置3の端末識別子および端末装置3に関係付けられたマッピングエージェントのIPv6アドレスを読み出し、端末装置1に送信する。端末装置1は、ドメインネームサーバ4から受信したマッピングエージェントのIPv6アドレスを基に、マッピングエージェントに端末装置3の端末識別子を示して、端末装置3の現在のネットワークプレフィックスを問い合わせる。マッピングエージェントは、端末装置3の端末識別子に対応して、端末装置3の現在のネットワークプレフィックスを送信する。これにより、端末装置3の現在のネットワークプレフィックスが得られる。

## 【0 1 2 7】

ステップS 6 7において、端末装置1は、ステップS 6 6の処理で取得されたネットワークプレフィックスが、図8の初期設定処理でハードディスクドライブ3 1に記憶されている端末装置3の最初のネットワークプレフィックスと同じで

あるか否かを判定する。

【0128】

ステップS67において、ステップS66の処理で取得されたネットワークプレフィックスが、ハードディスクドライブ31に記憶されている端末装置3の最初のネットワークプレフィックスと同じではないと判定された場合、ステップS68に進み、端末装置1のCPU21は、送信パケットの送信先アドレス（DESTINATION IP ADDRESS）の上位64ビットのdestination addressを、端末装置3の最初のネットワークプレフィックスに置換する。すなわち、送信先アドレスの上位64ビットのdestination addressには、端末装置3の最初のネットワークプレフィックスが記述される。

【0129】

ステップS67において、ステップS66の処理で取得されたネットワークプレフィックスが、ハードディスクドライブ31に記憶されている端末装置3の最初のネットワークプレフィックスと同じであると判定された場合、ステップS68の処理はスキップされる。

【0130】

ステップS69において、端末装置1のCPU21は、送信元アドレスの上位64ビットのsource addressに端末装置1の最初のネットワークプレフィックスを設定するとともに、送信先アドレスの上位64ビットのdestination addressに端末装置3の最初のネットワークプレフィックスを設定して、擬似ヘッダ（図11）を生成する。端末装置1のCPU21は、生成された擬似ヘッダに基づいて、認証データを演算し、演算された認証データを、送信パケットに格納する。

【0131】

ステップS70において、端末装置1のCPU21は、生成された擬似ヘッダ（図11）を用いて、TCP/UDPのチェックサムを演算する。演算結果（TCP/UDP LENGTH）は、送信パケットに格納される。

【0132】

ステップS71において、端末装置1のCPU21は、ステップS66の処理で取得された、端末装置3の現在の（最新の）ネットワークプレフィックスを、送

信パケットの送信先アドレスの上位64ビットに格納する。ステップS72において、端末装置1は、ステップS62の処理で取得された、自分の現在接続している（最新の）ネットワークのネットワークプレフィックスを、送信パケットの送信元アドレスの上位64ビットに格納する。

【0133】

ステップS73において、端末装置1のCPU21は、送信先アドレスに端末装置3の最新のネットワークプレフィックスが格納され、送信元アドレスに端末装置1の最新のネットワークプレフィックスが格納され、さらに、端末装置1の最初のネットワークプレフィックスと端末装置3の最初のネットワークプレフィックスを用いて演算された、認証データおよびTCP/UDPのチェックサム結果が格納された送信パケットを端末装置3に送信する。

【0134】

ステップS74において、端末装置1のCPU21は、アプリケーション層での通信が終了したか否かを判定し、アプリケーション層での通信が終了していないと判定した場合、ステップS62に戻り、上述したそれ以降の処理を繰り返す。そして、ステップS74において、アプリケーション層での通信が終了したと判定された場合、処理は終了される。

【0135】

このように、データパケットの送信時において、IP層の上位層に特別な変更を加えることなく、IPsec層およびトランスポート層（TCP/UDP）の移動透過性を保つことが可能となる。

【0136】

以上のように、IPルーティングを移動透過させるだけでなく、その上位層で行われるIPsecやTCP/IPのセッションの移動透過性も、既存のプロトコルを変更することなく実現することができる。

【0137】

また、以上においては、固定値やプライベート値を使用するといった、セッション専用のネットワークプレフィックスを定義する必要がなくなり、上位層であるTCP/UDPやIPsecの移動透過性を実現することができる。

## 【0138】

また、以上においては、ネットワークプレフィックスが変更されたか否かを判断することにより、変更された場合にのみ、認証データおよびチェックサムを演算するようにしたので、無意味なアドレス書き換えが行われなくて済む。

## 【0139】

さらにまた、以上においては、端末装置1が移動されたことを何らかの方法により知った場合、端末装置3は、再度、端末装置1のネットワークプレフィックスをマッピングエージェント81に問い合わせるようにしたが、例えば、移動するしないに関わらず、定期的に問い合わせるようにしてもよい。

## 【0140】

また、図10および図12の処理において、アプリケーション層での通信が再開されたか否かにより、それ以降の処理を行うようにしたが、本発明はこれに限らず、例えば、端末装置1と端末装置3との間で、SAによる鍵交換などが行われた場合に、それ以降の処理を行うようにしてもよい。

## 【0141】

さらにまた、図8に示した初期設定処理において、端末装置1および端末装置3のネットワークプレフィックスをハードディスクドライブ31に記憶する際に、端末装置1または端末装置3の移動が発生し、移動した先で異なる端末装置に対して新たにアプリケーションが起動される場合、それぞれのアプリケーションが最初に指定したネットワークプレフィックス (Source AddressとDestination Address) を、アプリケーションを指定するポート番号 (Source Port NumberとDestination Port Number) とともに記憶するようにしてもよい。

## 【0142】

上述した一連の処理は、ソフトウェアにより実行することもできる。そのソフトウェアは、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、記録媒体からインストールされる。

## 【0143】

この記録媒体は、図4または図5に示すように、コンピュータとは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク41または磁気ディスク61（フロッピーディスクを含む）、光ディスク42または光ディスク62（CD-ROM（Compact Disk-Read Only Memory）、DVD（Digital Versatile Disk）を含む）、光磁気ディスク43または光磁気ディスク63（MD（Mini-Disk）を含む）、もしくは半導体メモリ44または半導体メモリ64などよりなるパッケージメディアなどにより構成される。

#### 【0144】

なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

#### 【0145】

また、本明細書において、システムとは、複数の装置により構成される装置全体を表わすものである。

#### 【0146】

##### 【発明の効果】

本発明の第1の情報処理装置および方法、並びにプログラムによれば、他の情報処理装置との通信が確立したとき、情報処理装置の最初の位置を特定する第1の位置情報、および、他の情報処理装置の最初の位置を特定する第2の位置情報を記憶し、他の情報処理装置からデータを受信し、情報処理装置の現在の位置を特定する第3の位置情報を取得し、取得された第3の位置情報が第1の位置情報に対応するか否かを判定し、その判定結果に基づいて、受信されたデータを認証するようにしたので、データの受信時において、既存のプロトコルを変更することなく、IPsec層およびトランスポート層での移動透過性を実現することができる。

#### 【0147】

また、本発明の第2の情報処理装置および方法、並びにプログラムによれば、他の情報処理装置との通信が確立したとき、情報処理装置の最初の位置を特定す

る第1の位置情報、および、他の情報処理装置の最初の位置を特定する第2の位置情報を記憶し、情報処理装置の現在の位置を特定する第3の位置情報を取得し、取得された第3の位置情報が第1の位置情報に対応するか否かを判定し、他の情報処理装置の現在の位置を特定する第4の位置情報を取得し、取得された第4の位置情報が第2の位置情報に対応するか否かを判定し、それらの判定結果に基づいて、他の情報処理装置にデータを送信するようにしたので、データの送信時において、既存のプロトコルを変更することなく、IPsec層およびトランスポート層での移動透過性を実現することができる。

【図面の簡単な説明】

【図1】

本発明を適用したネットワークシステムの一実施の形態の構成例を示す図である。

【図2】

IPv6アドレスのフォーマット構造を示す図である。

【図3】

IPv6におけるプロトコル層の構成を示す図である。

【図4】

図1の端末装置の構成例を示すブロック図である。

【図5】

図1のルータの構成例を示すブロック図である。

【図6】

端末装置1と端末装置3との間のパケットデータのルーティング通信の動作を説明する図である。

【図7】

認証ヘッダのフォーマットを示す図である。

【図8】

初期設定処理を説明するフローチャートである。

【図9】

端末装置1の移動時の通信処理を説明するフローチャートである。

【図 1 0】

端末装置 1 の受信処理を説明するフローチャートである。

【図 1 1】

擬似ヘッダのフォーマットを示す図である。

【図 1 2】

端末装置 1 の送信処理を説明するフローチャートである。

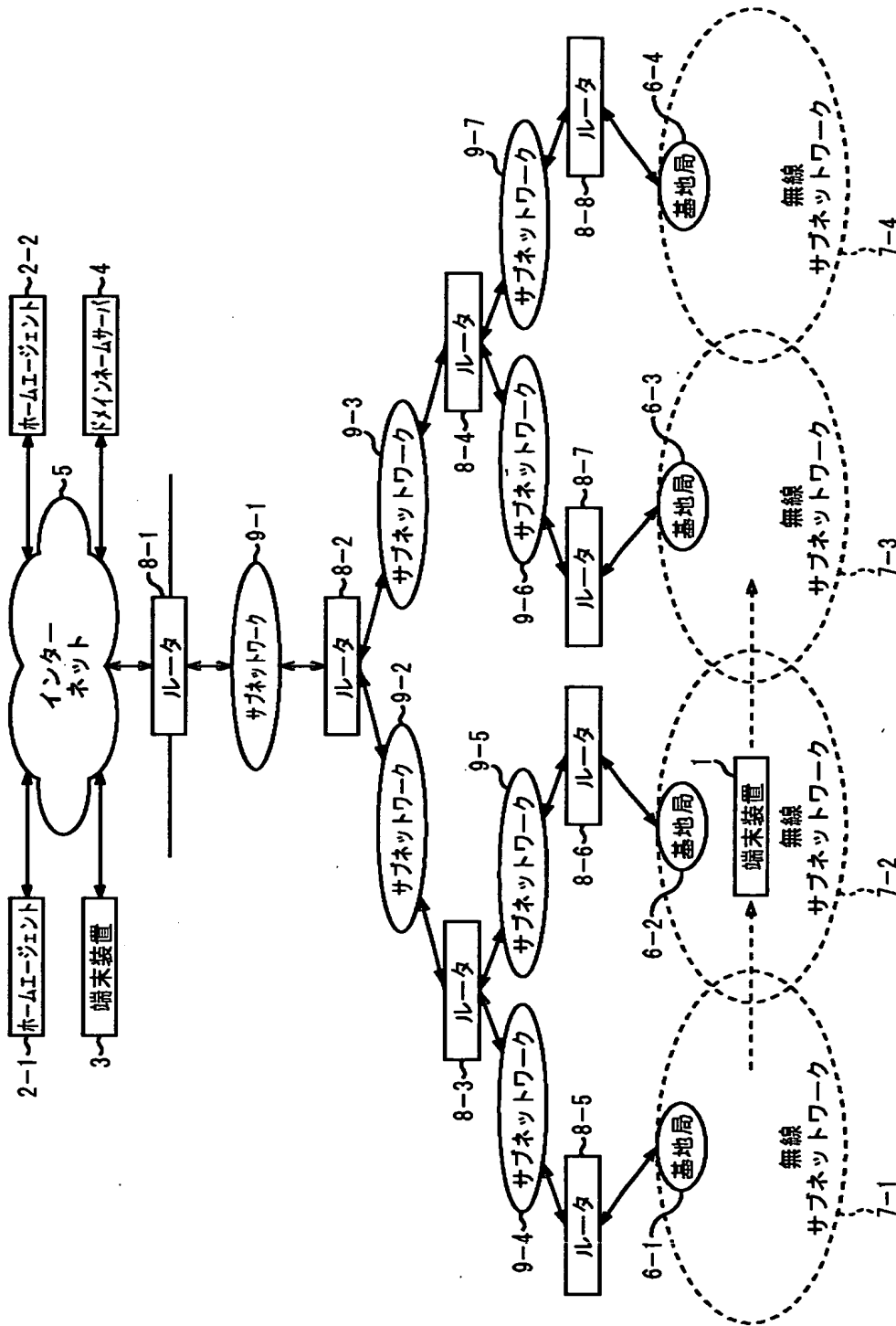
【符号の説明】

1, 3 端末装置, 4 ドメインネームサーバ, 8-1 乃至 8-8 ルータ, 21 CPU, 22 ROM, 23 RAM, 31 ハードディスクドライブ, 33 通信部, 41 磁気ディスク, 42 光ディスク, 43 光磁気ディスク, 44 半導体メモリ, 61 磁気ディスク, 62 光ディスク, 63 光磁気ディスク, 64 半導体メモリ, 81 マッピングエージェント

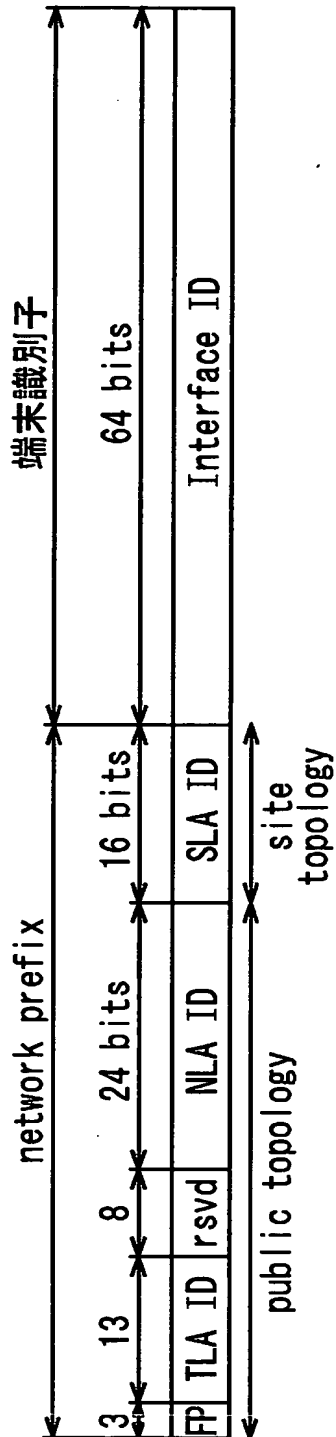


【書類名】図面

【図1】



【図 2】



【図3】

TCP/UDP・アプリケーション層

64bit

ネットワーク  
プレフィックス

TCP  
Connection  
↔

IPsec層

64bit

ネットワーク  
プレフィックス

IP sec SA  
↔

IP層

64bit

ネットワーク  
プレフィックス

64bit

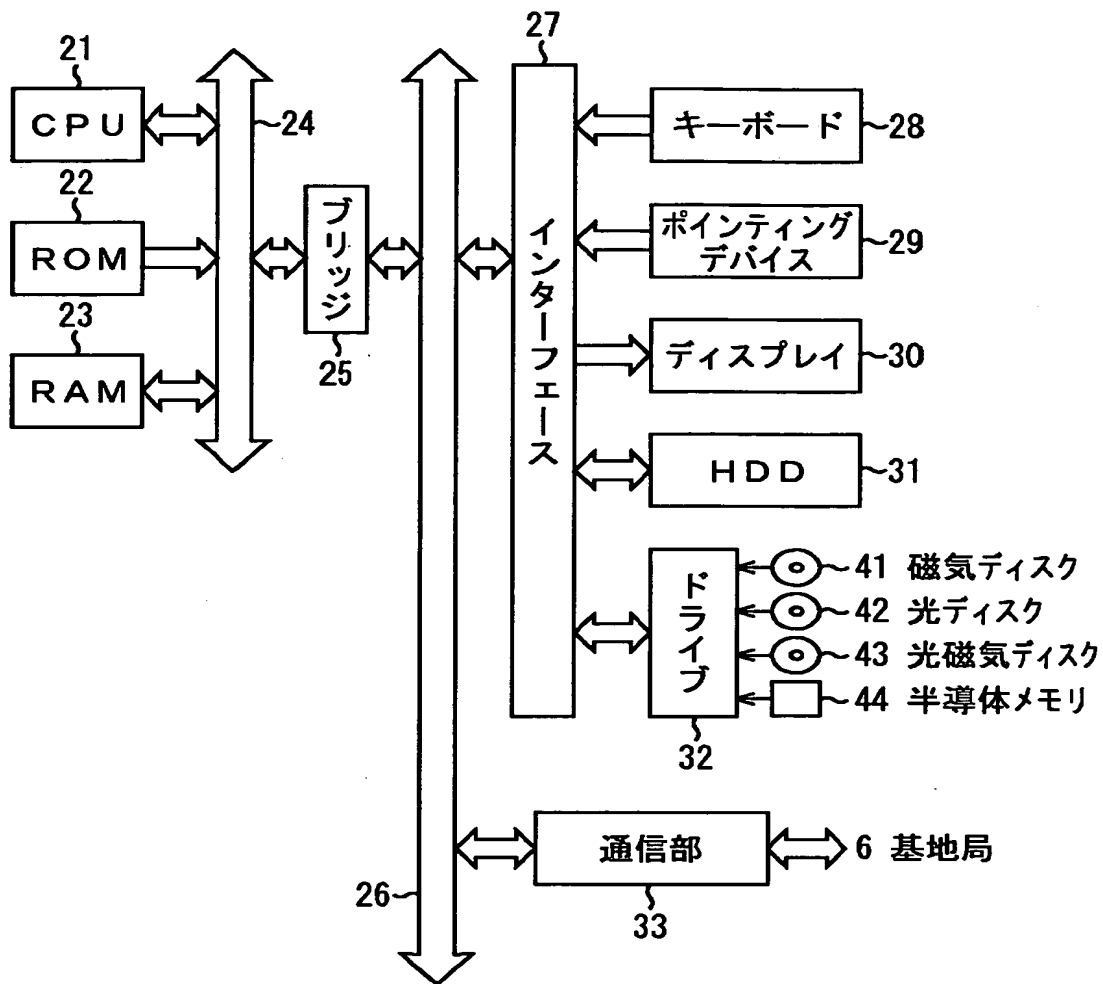
端末識別子

データリンク・物理層

128bit

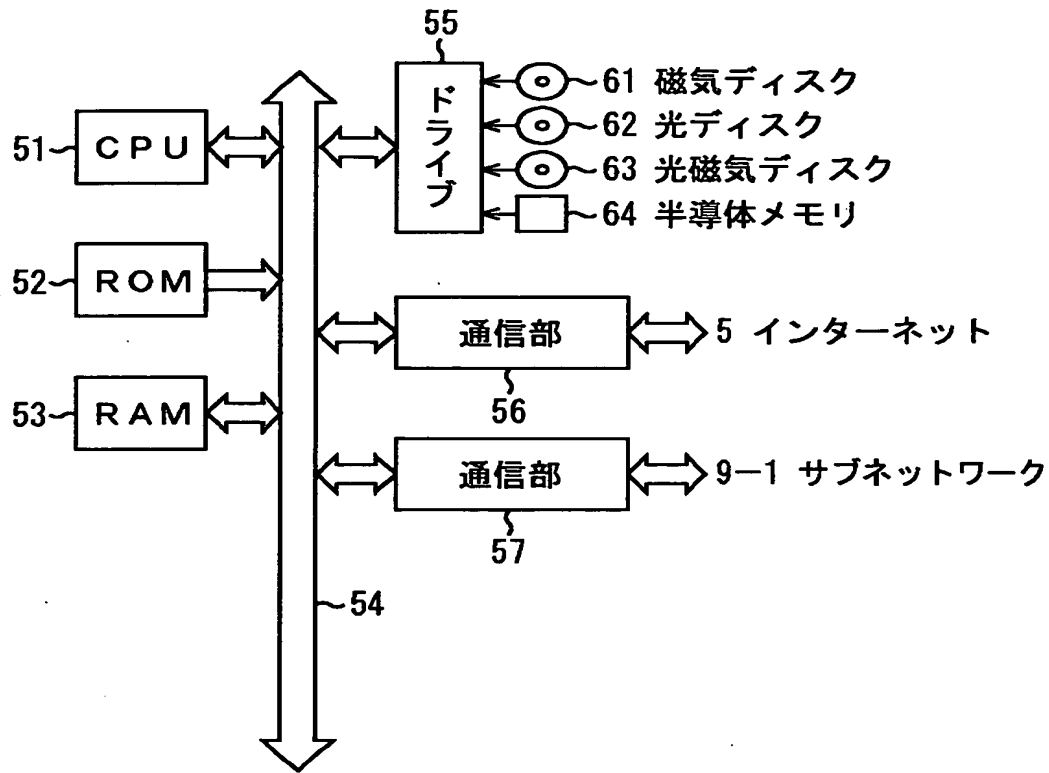
IPv6アドレス

【図 4】



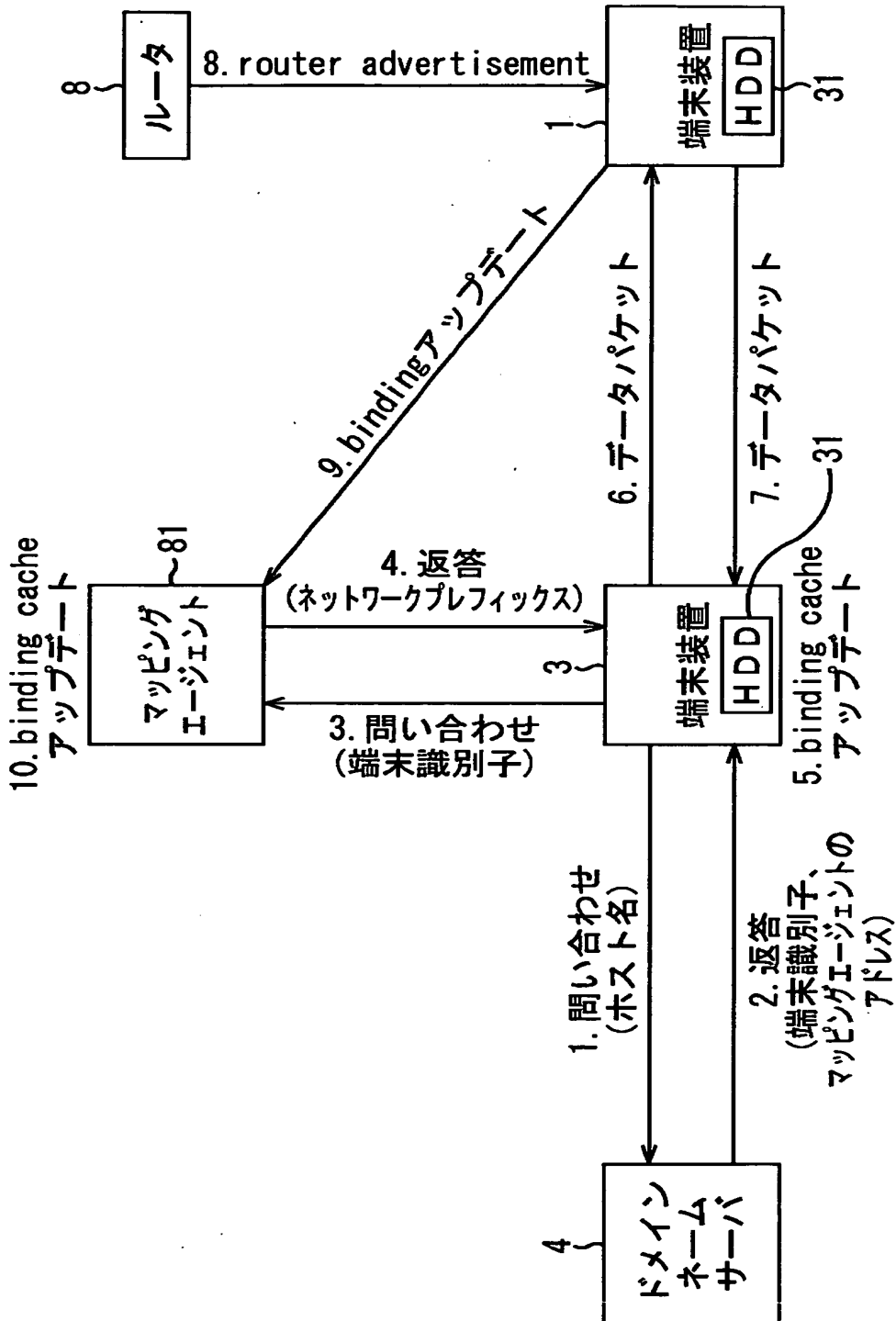
端末装置 1

【図 5】

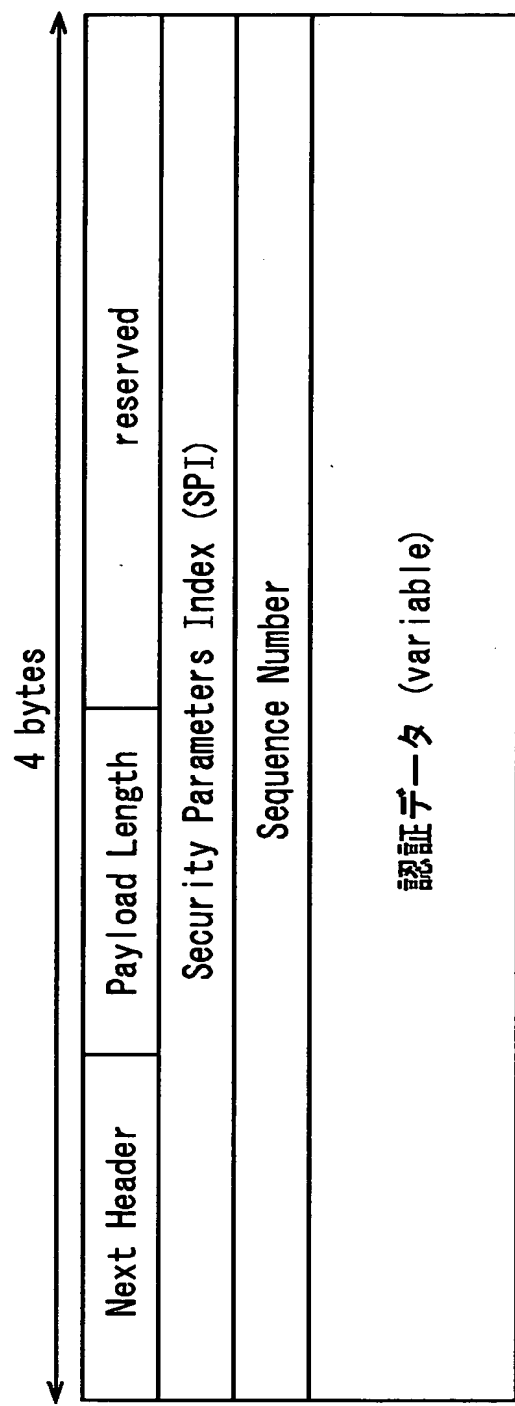


ルータ 8-1

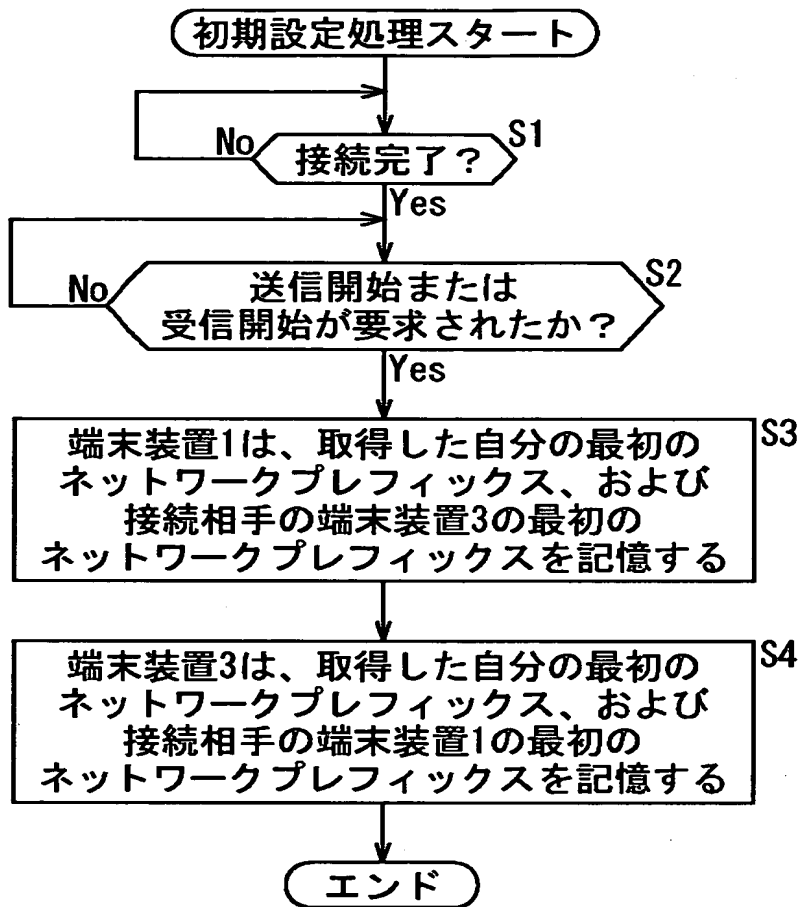
【図 6】



【図7】

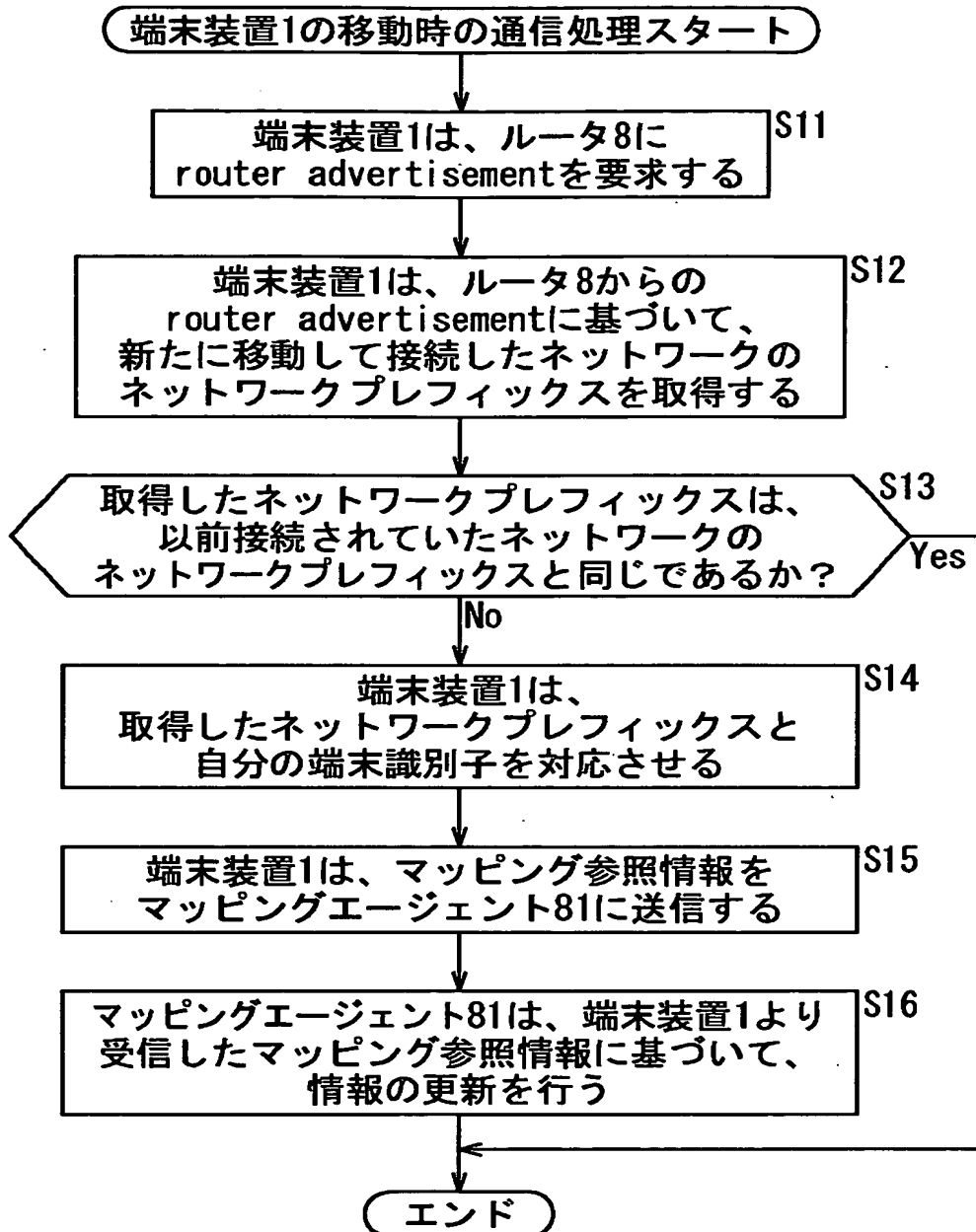


【図8】

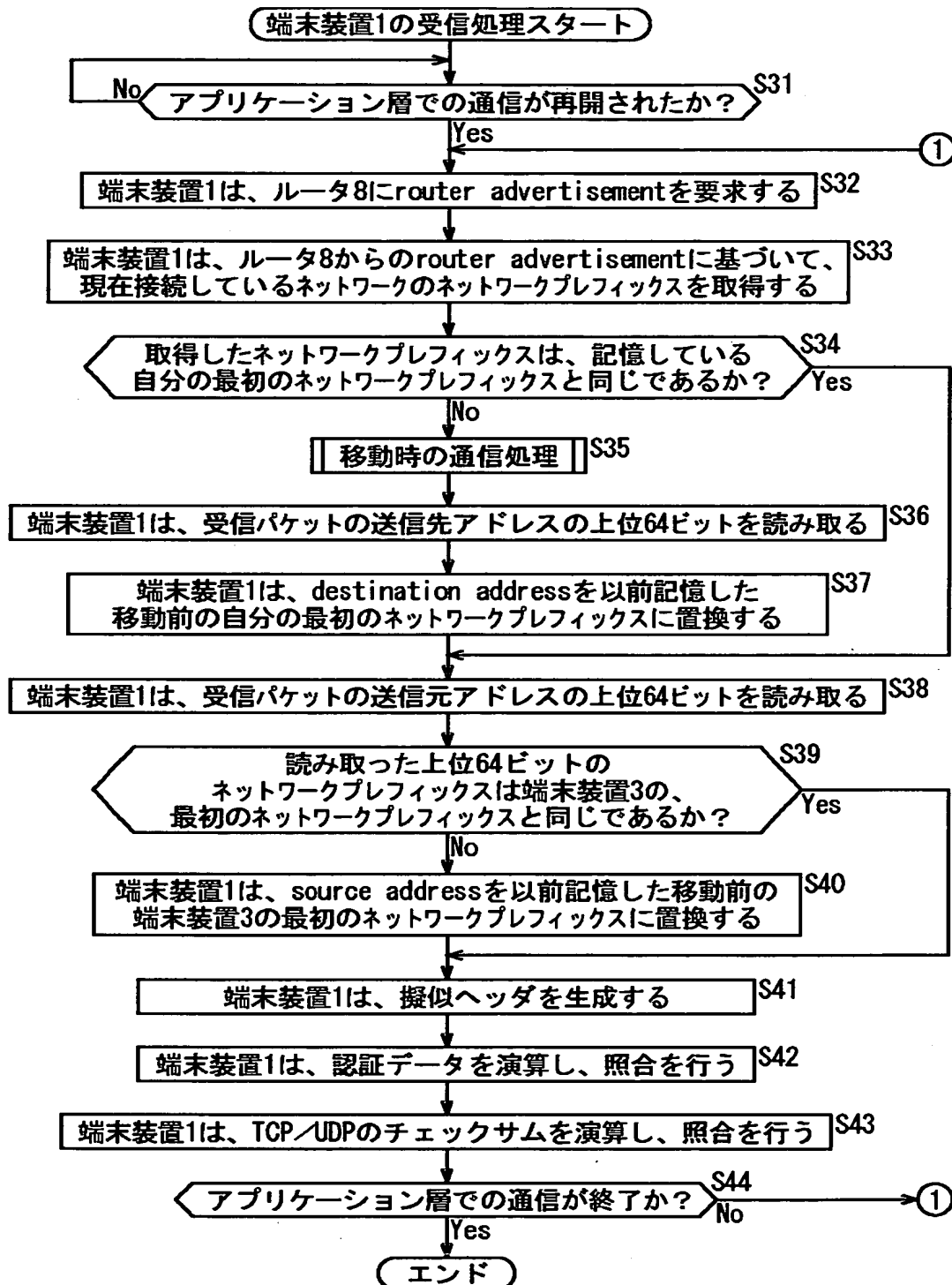




【図 9】



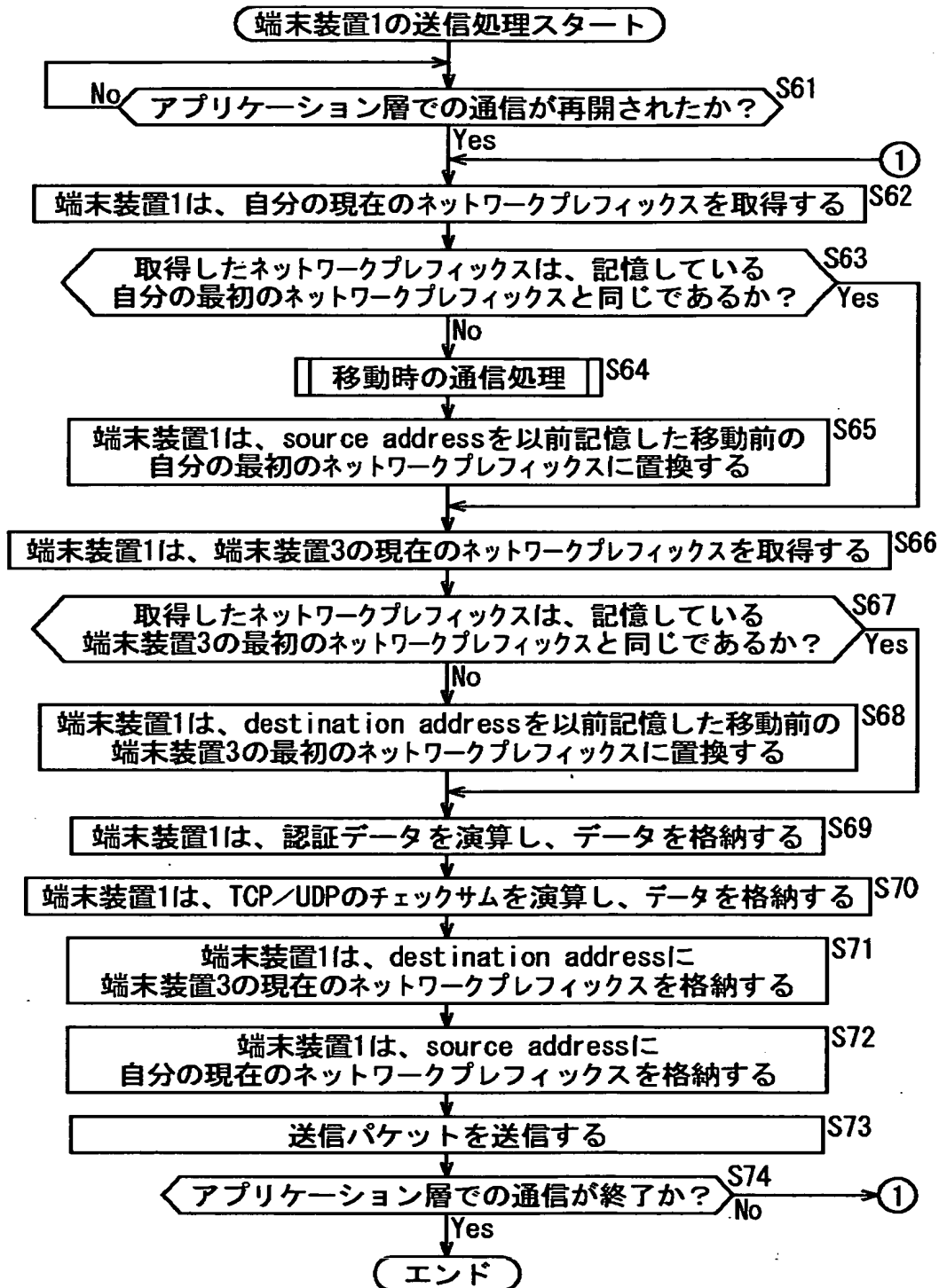
【図 10】



【図 1 1】

SOURCE IP ADDRESS	
DESTINATION IP ADDRESS	
ZERO	TCP/UDP LENGTH

【図 12】



【書類名】 要約書

【要約】

【課題】 上位層での移動透過性を実現することができるようにする。

【解決手段】 端末装置 1 は、ステップ S 3 3, 3 4 において、自分が現在接続しているネットワークのネットワークプレフィックスを取得し、それが最初のネットワークプレフィックスと同じであるか否かを判定し、異なる場合、ステップ S 3 5 乃至 S 4 1 において、受信パケットの送信先アドレスおよび送信元アドレスのネットワークプレフィックスをそれぞれ読み取り、その読み取ったネットワークプレフィックスが、最初のネットワークプレフィックスと異なる場合、最初のネットワークプレフィックスに置換して、擬似ヘッダを生成する。そして、端末装置 1 は、ステップ S 4 2, S 4 3 において、生成された擬似ヘッダを用いて、受信パケットの認証を行う。

【選択図】 図 1 0

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日	1990年 8月30日
[変更理由]	新規登録
住 所	東京都品川区北品川6丁目7番35号
氏 名	ソニー株式会社